ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

An Efficient Password Security Mechanism Using Two Server Authentication and Key Exchange

Pooja Kolte[1]
Dept. of Information Tech
NMIET
Pune, India

Reshma Gutal[2]
Dept. of Information Tech
NMIET
Pune, India

Priyanka Bhairat[3]
Dept. of Information Tech
NMIET
Pune, India

Abstract: User Authentication in computer systems is an important cornerstone in today's computer era. The concept of a user id and password is one of the easiest ways for authentication. It is not only the easiest way, but also cost effective and highly efficient. Today, we can see the password cracking and hacking in everywhere. At present we are using the single server system for this sort of password based authentication. Traditional protocols for password-based authentication assume a single server which stores all the information (e.g., the password) necessary to authenticate a user. When an attacker obtains the information stored on the server, he can obtain all the passwords which were stored in the server via launching an off-line dictionary attack. To address this issue, a number of schemes have been proposed in which a user's password information is shared among multiple servers, and these servers cooperate to authenticate the user. In this paper, a new efficient two-server password-only based authentication is proposed where the client can establish different cryptographic keys with the two servers. These two servers' runs parallel and collude with each other to authenticate the user.

Keywords: Diffie-Hellman Key Exchange, ElGamal Encryption Scheme, PAKE Protocol, Cryptography, Password Security Mechanism, Two server concept.

I. Introduction

Password based user authentication systems are low cost and easy to use. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access devices he/she employs. A user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers', accessing programs, databases, networks, web sites, and even reading the morning newspaper online.

Traditional protocols for password-based authentication assume a single server which stores all the information (e.g., the password) necessary to authenticate a user. Password based authentication is the most commonly used entity authentication technique, due to the fact that no secure storage is required, and a user only needs to memorize his password and then can authenticate anywhere, anytime. Most of the existing password based authentication schemes assume the single-server model where a single server exists in a system. The major drawback of the single server model is that the server may result in a single point of failure, in the sense that compromise of the server reveals all user passwords held by the server. The server is compromised by means of an offline dictionary attack. To solve this problem, a new kind of authentication structure called the multiple server authentication was proposed. In such schemes, the capability of verifying a password is split between two or more servers, and these servers need to collude to recover the password.

In this paper, we propose a new symmetric solution for two-server PAKE. An efficient security mechanism is proposed for authenticating the users. The proposed system use the concept of public key cryptosystem and follows the password-only model. The proposed system makes use of the two server concept along with Diffie-Hellman Key Exchange algorithm and ElGamal encryption scheme.

II. Preliminaries

Diffie-Hellman Key Exchange Protocol

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. Consider two users Alice and Bob, who wish to exchange a secret key between them. Diffie-Hellman key exchange algorithm works as follows:

1. Alice and Bob agree on a cyclic group G of large prime order q with a generator g.

2. Alice randomly chooses an integer a from Z*q and computes $X = g^a$. Alice sends X to Bob.

3. Bob randomly chooses an integer b from Z*q and computes $Y = g^b$. Bob sends Y to Alice.

4. Alice computes the secret key $k1 = Y^a = g^{ba}$.

5. Bob computes the secret key $k2 = X^b = g^{ab}$.

It is concluded that k1 = k2 and thus Alice and Bob have agreed on the same secret key, by which the subsequent communications between them can be protected.Diffie-Hellman key exchange protocol is secure against any passive adversary, who cannot interact with Alice and Bob, attempting to determine the secret key solely based upon observed data.

ElGamal Encryption Algorithm

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. The algorithm consists of three phases: key generation, encryption, and decryption.

ElGamal Encryption Algorithm works as follows:

1. Key Generation:

Participant A generates the public/private key pair

a. Generate large prime p and generator g of the multiplicative Group Z*p of the integers modulo p.

b. Select a random integer a, $1 \leq a \leq p - 2$, and compute ga mod p.

c. A’s Public key is (p, g, g^a). A’s Private key is a.

2. Encryption:

Participant B encrypts a message m to A

a. Obtain A’s authentic public key (p, g, g^a).

b. Represent the message as integer’s m in the range

{0, 1, 2, ……….., p-1}

c. Select a random integer k, $1 \leq k \leq p - 2$.

d. Compute $\gamma = g^k \bmod p$ and $\delta = m * (g^a)^k$

e. Send cipher text $c = (\gamma, \delta)$ to A.

3. Decryption

Participant A receives encrypted message m from B

a. Use private key a to compute $(\gamma^{p-1-a}) \bmod p$.

b. Recover m by computing $(\gamma^{-a}) * \delta \bmod p$.

III. Proposed System

In our system, there exist two servers. The two servers cooperate and provide services to authenticated clients. Client chooses password and cannot authenticate unless both the servers collude. The two servers cooperate to authenticate the client. In our protocol, the client and the two servers communicate through a public channel.

The following diagram shows the architecture of the system:

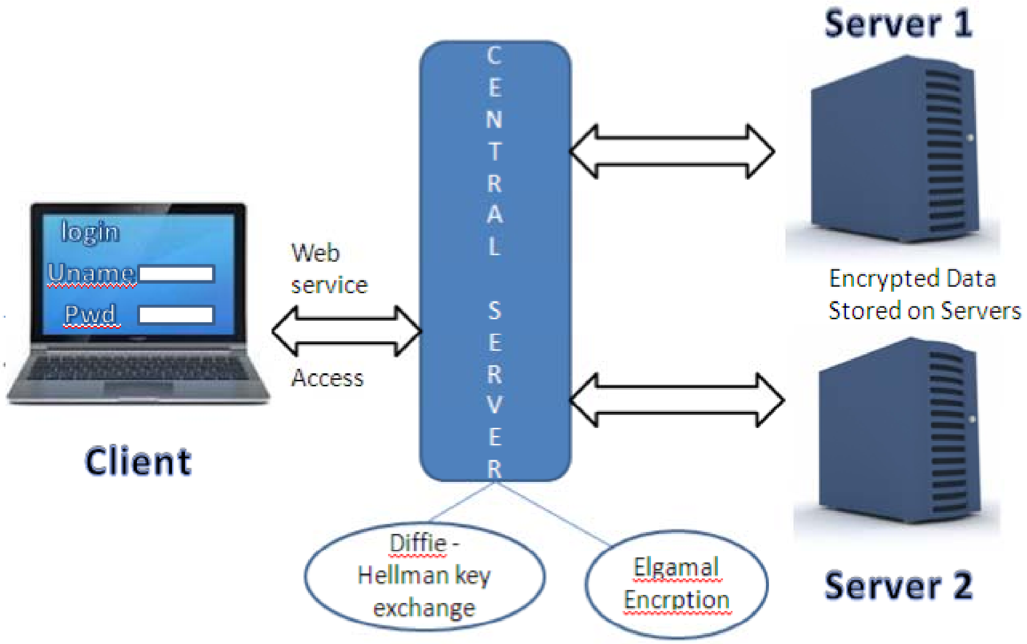

Fig.1. System Architecture

In our system, there exist two servers S1 and S2 and a group of clients. The two servers cooperate to authenticate clients and provide services to authenticated clients. Prior to authentication, each client C chooses a password pwC and generates the password authentication information AuthC(1) and AuthC(2) for S1 and S2, respectively, such that nobody can determine the password pwC from AuthC(1) or AuthC(2) unless S1 and S2 collude. The client sends AuthC (1) and AuthC (2) to S1 and S2, respective, through different secure channels during the client registration. After that, the client remembers the password only, and the two servers keep the password authentication information. The authentication information is stored on both servers in encrypted form using ElGamal Algorithm. When the client performs login operation the central server requests for the authentication information from both servers. Both the servers decrypt their part of authentication information and send it to central server. The authentication information is merged at central server. If merged information and the password entered by the client matches then the particular client is authenticated.

IV. Conclusion

In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Thus an efficient authentication mechanism is proposed in this paper. The proposed system is very efficient as compared to the traditional authentication protocols implemented on single server. The involvement of more than one server increases the security of authentication process and prevents our system from active and passive attacks.

Acknowledgment

This work is supported by assistant professor Mr.Pramod Patil and assistant professor Mr. Prasad Chaudhari.We would like to thank them for their guidance and help.

References

1. Xun Yi, San Ling, and Huaxiong Wang “Efficient Two-Server Password-Only Authenticated Key Exchange”, IEEE – 2013
2. Vignesh Kumar K, Angulakshmi T, Manivannan D, Seethalakshmi R, Swaminathan P “Password Based Two Server Authentication System”, JATIT - 2012
3. Mihir Bellare, David Pointcheval and Phillip Rogaway “Authenticated Key Exchange Secure Against Dictionary Attacks”.
4. Michel Abdalla. David Pointcheval “Simple Password-Based Encrypted Key Exchange Protocols”.
5. Steven M. Bellovin, Michael Merritt “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”.
6. M. Abdalla, O. Chevassut, and D. Pointcheval, “One-Time Verifier-Based Encrypted Key Exchange,” Proc. Eighth Int’l Conf. Theory and Practice in Public Key Cryptography - 2005.
7. D. Boneh and M. Franklin, “Identity Based Encryption from the Weil Pairing,” SIAM J. Computing - 2003.